REMARKS

Claims 1-16 and 33-46 are currently pending in this application. Claims 17-32 were previously cancelled without prejudice or disclaimer. Claims 1, 2, 16, 33-35 and 38-40 have been amended and claims 42-44 have been canceled by way of the present amendment.

In the outstanding Office Action, claims 1-16, 42 and 46 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement; claims 1-16, 42 and 45 stand rejected under 35 U.S.C. §112, second paragraph; claims 1-3, 5-6, 33-35, 37-40 and 42-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by "RFC 2328 – OSPF Version 2"(Moy); claims 1-6, 33-35, 37-40 and 42-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by "Digital Signature Protection of the OSPF Routing Protocol" (Murphy et al.) as evidence by Moy; claims 1-8, 10-12 and 33-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2002/0016926 (Nguyen et al.) as evidence by Moy; claims 13-15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen et al. as evidence by Moy and further in view of U.S. Patent No. 7,103,185 (Srivastava et al.); claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen et al. as evidence by Moy and further in view of U.S. Patent No. 6,085,320 (Kaliski, Jr.); and claim 16 was not rejected over the prior art.

Allowable Subject Matter

First, Applicants would like to thank Examiner Dinh for the early indication of allowable subject matter in the form of dependent claim 16. To that end, the limitations of base claim 1, including amendments to overcome the outstanding rejections under 35 U.S.C. §112, have been incorporated into allowable claim 16 and thus, it is respectfully submitted that claim16 is in condition for allowance.

Rejections Under 35 U.S.C. §112

Claims 1-16, 42 and 46 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. Reconsideration is respectfully requested.

The outstanding Office Action has requested that, in order to overcome the 35 U.S.C. §112, first paragraph, rejection, the following items should be shown: (i) how the receiver determines the a random value to be used; (ii) how this random value is related to the random value used by the signer; (iii) what are the specific two different functions used by the signer and the receiver; (iv) proof showing that these two functions generate the same digital signature. The following paragraphs are in response to that request.

With regard to item (i), it is respectfully submitted that the specification discloses a "random value or *time stamp* may be used for verification of the digital signature DS" (emphasis added), and thus, the receiver would determine a "time stamp" from a clock/time source accessible by the receiver. Support for this definition is provide at least in **paragraph [0050]** and shown at least in **FIG. 3**, **FIG. 4A** and **FIG. 4B** of the specification. Further, with respect to item (ii), in consideration of the above discussion, the random values/time stamps are each determined by a clock/time source and thus, each are related to one another by the difference-in-time between when each of the random values/time stamps are created. In addition, it is respectfully submitted that the specification explicitly discloses the concept of differentiating information based on timestamp in that it recites:

> **[0050]** [*T*]*he random value or time stamp may be used for verification of the digital signature DS.* The time stamp, if included in the packet, can further be *used by other nodes for checking whether a received jump-start packet is a recent packet and not an old packet* to be disregarded.

With regard to item (iii), it is assumed that the outstanding Office Action is referring to the encryption "function" that occurs during an exchange of messages between routers, as discussed in paragraphs **[0051]** to **[0056]** of the published application. It is respectfully submitted that at least one method for performing the encryption function is disclosed in paragraph **[0083]** to **[0084]** of the published application, as recited below:

> **[0083]** ...The DR uses its public/private key pair and determines a random session key. This session key *can be generated by several schemes. One possible way is to generate the key as follows: Key=Hash(Random Number, private Key, Public Key, TimeStamp).*
> **[0084]** This key is used as credential and is applied on the hello packet either for *authentication or encryption* (emphasis).

In regards to item (iv), the following section of an article entitled: Search.Security.com Definitions," which can be obtained from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html defines a Public Key Infrastructure (PKI) asdiscloses:

> **How Public and Private Key Cryptography Works**
>
> In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. *The private key is never shared with anyone or sent across the Internet* (emphasis added). You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory).
>
> Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. *In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital certificate. When I receive it, I can use your public key to decrypt it* (emphasis added).

Here's a table (emphasis added) that restates it:

To do this	**Use whose**	**Kind of key**
Send an encrypted message	Use the receiver's	Public key
Send an encrypted signature	*Use the sender's*	*Private key*
Decrypt an encrypted message	Use the receiver's	Private key
Decrypt an encrypted signature (and authenticate the sender)	*Use the sender's*	*Public key*

That is, as discussed in the article and table above, in order to: "send an encrypted signature" (i.e., DS**1**), one uses the sender's "private key," (i.e., *see* "Private Key of Router **1**") as disclosed in paragraph **[0052]** of the published specification; and to "decrypt an encrypted signature (and authenticate the sender)" one uses the senders "public key," (i.e., *see* "Public Key of Router 1") as disclosed in paragraph **[0054]** of the published specification, to decrypt and authenticate the encrypted signature (i.e., DS**2**). Thus, the same digital signature generated by DS**1** can be detected and authenticated by DS**2**, when, as recited in claims:

> receiving the jump-start message at a receiving node;
> validating an authenticity of the jump-start message upon receipt of the start message at the receiving node.

Therefore, in view of the above discussion, withdrawal of this outstanding rejection is respectfully requested.

Claims 1-16, 42 and 45 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Reconsideration is respectfully requested.

Claim 1 has been amended to clarify the invention. In particular, claim 1 has been amended, as suggested in the outstanding Office Action, to recite:

> providing a specific multicast channel for sending jump-start messages by ~~the nodes~~ a node to ~~said~~ other nodes when ~~a~~ the node has not received any regular start-up messages from said other nodes on one or more multicast channels used for regular start-up messages.

Thus, it is respectfully submitted that the claims are now definite and it is requested that the outstanding rejection be withdrawn.

Rejections Under 35 U.S.C. §102

Claims 1-3, 5-6, 33-35, 37-40 and 42-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by Moy. Reconsideration is respectfully requested.

Claim 1 has been amended to clarify the invention. In particular, claim 1 has been amended to recite:

> providing two multicast channels for exchanging regular start-up messages including at least a hello packet and a Link State Advertisement (LSA) summary;
>
> providing a ~~specific~~ third multicast channel for sending jump-start messages by ~~the nodes~~ a node to ~~said~~ other nodes when ~~a~~ the node has not received any regular start-up messages from said other nodes on one or more multicast channels used for regular start-up messages.

Independent claims 33 and 38, and various dependent claims have also been amended similarly. Support for the amendments is provided at least at paragraphs **[0034]** to **[0037]** and shown at least in **FIG. 3**. Thus, the amendment raises no questions of new matter.

Moy discloses an Open Shortest Paths First (OSPF) protocol that routes Internet Protocol packets based solely on the Intenet Protocol (IP) address of the packet header.[1] In particular, in paragraph **8**, the outstanding Office Action states Moy discloses:

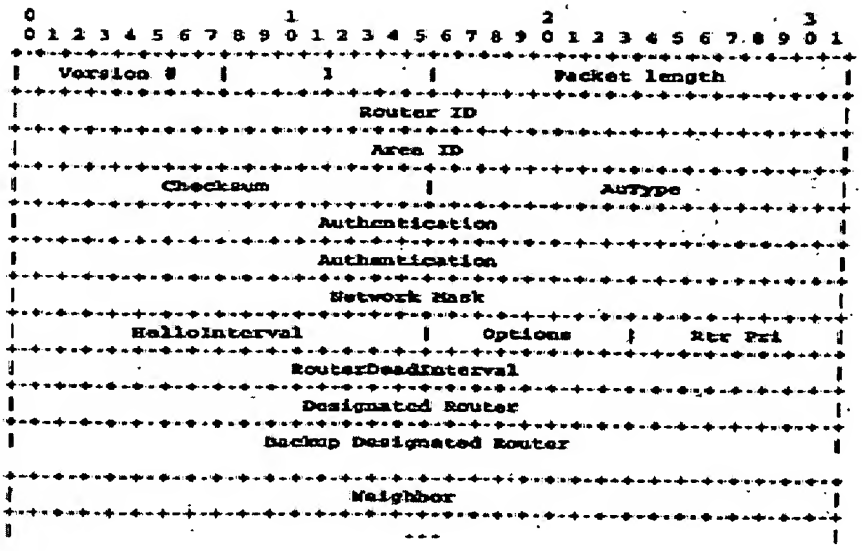
> [T]he Hello message allows a neighboring router(s) to update its information regarding the status of the starting router (i.e., from previously Down) and to establish adjacency between the routers (page 50, Section 10.1, Neighbor States). Therefore, the Hello message is *functionally equivalent to a jump-start message*.

However, Moy nowhere discloses as claim 1 has been amended to recite:

> *providing two multicast channels for exchanging regular start-up messages including at least a hello packet and a Link State Advertisement (LSA) summary*;
> *providing a third multicast channel for sending jump-start messages by a node to other nodes when the node has not received any regular start-up messages* from said other nodes on one or more multicast channels used for regular start-up messages (emphasis added).

Independent claims 33 and 38 recite similar limitations. That is, Moy discloses the regular-start-up messages such as a Hello Packet, it nowhere discloses the recited: "jump-start message" or "a third multicast channel" that transmits the "jump-start message." In addition, Moy discloses the "Hello Packet," as discussed in **Section A.3.2** and as shown in the figure from that section below.

[1] Moy at page 54, Section: Introduction.



In contrast to the "Hello Packet" as shown above and disclosed by Moy, claim 1 recites a "jump-start packet" as is shown in **FIG. 3** of the published application below:

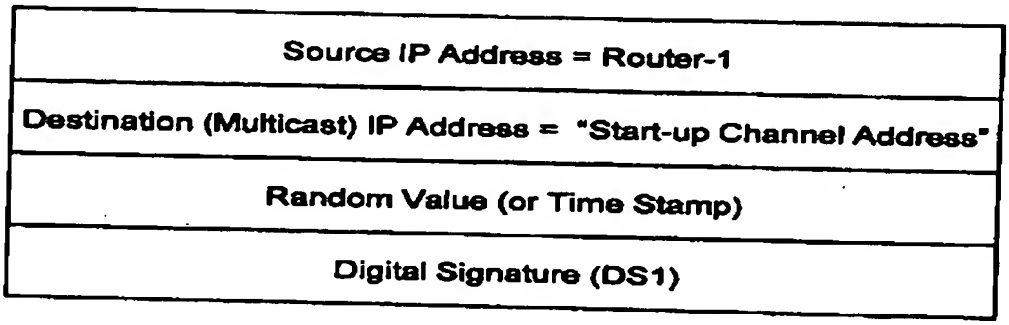


FIG. 3

JUMP-START PACKET

Further, it is respectfully submitted that the disclosure of the published specification clearly teaches away from the "Hello Message" of the background art of Moy. In particular, the specification clearly discloses:

> **[0035]** ...[T]he router may begin with a jump-start mechanism *instead of sending out its Hello packets* (emphasis added). ....
>
> **[0036]** Before sending an initiating message, e.g. a hello packet, each OSPF router R1 to R6 has to know what keys and credentials have to be applied to the hello packet. For OSPF, hello packet is normally the first message generated by the OSPF nodes so there is no way to find out the other legitimate nodes in the current OSPF shared segment. This is called a live lock situation, where the OSPF routers want to send the hello packet, but to generate hello packet OSPF, the OSPF routers have to know what keys and credentials to be applied to that packet so that other nodes can authenticate the hello packet.
>
> **[0037]** *To solve this live lock problem, in at least one or more or all of the described embodiments of the invention when the OSPF application process is started, the hello packets are not, or need not be exchanged as the first packets.* (emphasis added).

Therefore, it is respectfully submitted that Moy does not disclose, anticipate or inherently teach the claimed invention and that independent claims 1, 33 and 38, and claims dependent thereon, patenably distinguish thereover.

Claims 1-6, 33-35, 37-40 and 42-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by Murphy et al. as evidence by Moy.

As discussed above, Moy does not disclose the claimed invention. Thus, it is respectfully submitted that Moy also does not "evidence" the claimed invention. Murphy et al. discloses routing protocols for distributing information regarding topology of the network among the routers of the network.[2] In particular, Murphy et al. discloses adding digital signatures to OSPF LSA data, and recommend the use of neighbor-to-neighbor authentication.

[2] Murphy et al. at Introduction.

However, Murphy et al. nowhere discloses as claim 1 has been amended to recite:

> providing two multicast channels for exchanging regular start-up messages including at least a hello packet and a Link State Advertisement (LSA) summary;
> *providing a third multicast channel for sending jump-start messages by a node to other nodes when the node has not received any regular start-up messages* from said other nodes on one or more multicast channels used for regular start-up messages (emphasis added).

Independent claims 33 and 38 recite similar limitations. That is, Murphy et al. nowhere discloses the recited: "jump-start message" or "a third multicast channel" that transmit the "jump-start message." Therefore, it is respectfully submitted that Moy does not evidence and Murphy et al. does not disclose, anticipate or inherently teach the claimed invention and that independent claims 1, 33 and 38, and claims dependent thereon, patenably distinguish thereover.

Claims 1-8, 10-12 and 33-46 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2002/0016926 Nguyen et al. as evidence by Moy.

As discussed above, Moy does not disclose the claimed invention. Thus, it is respectfully submitted that Moy also does not "evidence" the claimed invention. Nguyen et al. discloses a group of Secure Gateway Devices is connected between their respective local area networks, and a public network (such as the internet); the Secure Gateway Devices create a cloud of virtual gateways that are all located at the same virtual IP address; and that in this network, standard routing protocols are used by network devices to pass their routing information.[3] However, Nguyen et al. nowhere discloses as claim 1 has been amended to recite:

> providing two multicast channels for exchanging regular start-up messages including at least a hello packet and a Link State Advertisement (LSA) summary;
> *providing a third multicast channel for sending jump-start messages by a node to other nodes when the node has not received any regular start-up messages* from said other nodes on one or

[3] Nguyen et al. at ABSTRACT.

> more multicast channels used for regular start-up messages (emphasis added).

Independent claims 33 and 38 recite similar limitations. That is, Nguyen et al. nowhere discloses the recited: "jump-start message" or "a third multicast channel" that transmit the "jump-start message." Therefore, it is respectfully submitted that Moy does not evidence and Nguyen et al. does not disclose, anticipate or inherently teach the claimed invention and that independent claims 1, 33 and 38, and claims dependent thereon, patenably distinguish thereover.

Rejections Under 35 U.S.C. §103

Claims 13-15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen et al. as evidence by Moy and further in view of Srivastava et al.

Claims 13-15 are ultimately dependent upon claim 1. As discussed above, Moy does not disclose the claimed invention and Moy also does not "evidence" the claimed invention. In addition, as discussed above, Nguyen et al. also does not disclose the claimed invention. The outstanding Office acknowledges deficiencies in both Moy and Nguyen et al. and attempts to overcome those deficiencies by combining Srivastava et al. with the references. However, Srivastava et al. cannot overcome all of the deficiencies of the discussed references, as discussed below.

Srivastava et al. discloses an approach for establishing secure multicast communication among multiple multicast proxy service nodes.[4] network devices to pass their routing information.[5] However, Srivastava et al. nowhere discloses as claim 1 has been amended to recite:

[4] Srivastava et al. at ABSTRACT.
[5] Nguyen et al. at ABSTRACT.

> providing two multicast channels for exchanging regular start-up messages including at least a hello packet and a Link State Advertisement (LSA) summary;
> *providing a third multicast channel for sending jump-start messages by a node to other nodes when the node has not received any regular start-up messages* from said other nodes on one or more multicast channels used for regular start-up messages (emphasis added).

Independent claims 33 and 38 recite similar limitations. That is, Sravistava et al. nowhere discloses the recited: "jump-start message" or "a third multicast channel" that transmit the "jump-start message." Therefore, it is respectfully submitted that Moy does not evidence and neither Nguyen et al. nor Sravistava et al. disclose, suggest or make obvious the claimed invention and that independent claims 1, 33 and 38, and claims dependent thereon, patenably distinguish thereover.

Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen et al. as evidence by Moy and further in view of Kaliski, Jr.

Claims 13-15 are ultimately dependent upon claim 1. As discussed above, Moy does not disclose the claimed invention and Moy also does not "evidence" the claimed invention. In addition, as discussed above, Nguyen et al. also does not disclose the claimed invention. The outstanding Office acknowledges deficiencies in both Moy and Nguyen et al. and attempts to overcome those deficiencies by combining Kaliski, Jr. with the references. However, Kaliski, Jr. cannot overcome all of the deficiencies of the discussed references, as discussed below.

Kaliski, Jr. discloses a protocol for establishing the authenticity of a client to a server in an electronic transaction by encrypting a certificate with a key known only to the client and the server.[6] However, Kaliski, Jr. nowhere discloses as claim 1 has been amended to recite:

> providing two multicast channels for exchanging regular start-up messages including at least a hello packet and a Link State Advertisement (LSA) summary;

[6] Kaliski, Jr. at ABSTRACT.

> *providing a third multicast channel for sending jump-start messages by a node to other nodes when the node has not received any regular start-up messages* from said other nodes on one or more multicast channels used for regular start-up messages (emphasis added).

Independent claims 33 and 38 recite similar limitations. That is, Kaliski, Jr. nowhere discloses the recited: "jump-start message" or "a third multicast channel" that transmit the "jump-start message." Therefore, it is respectfully submitted that Moy does not evidence and neither Nguyen et al. nor Kaliski, Jr. disclose, suggest or make obvious the claimed invention and that independent claims 1, 33 and 38, and claims dependent thereon, patenably distinguish thereover.

Conclusion

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

The Office is authorized to charge any necesssary fees to Deposit Account No. 22-0185.

Applicant believes no fee is due with this response. However, if a fee is due, please

charge our Deposit Account No. 22-0185, under Order No. 27592-00454-US from which the undersigned is authorized to draw.

Dated: June 25, 2008

Respectfully submitted,

Electronic signature: /Myron K. Wyche/
Myron K. Wyche
Registration No.: 47,341
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Agent for Applicant